SECTION XIV. ROUTINE DESTRUCTION OF COMSEC MATERIAL

97. General. The security achieved through the proper use of contemporary U.S. cryptosystems is heavily dependent upon the physical protection which is afforded the associated keying material. Current and superseded keying material is extremely sensitive, since its compromise potentially exposes to compromise all traffic encrypted with it. For this reason, keying material (other than defective or faulty key) 1/ must be destroyed as soon as possible after it has been superseded or has otherwise served its intended purpose. Destruction of superseded or obsolete crypto-equipment and supporting documentation is also essential to the maintenance of a satisfactory national COMSEC posture, since these materials may be of significant long-term benefit to hostile interests desiring to exploit U.S. communications for intelligence purposes.

98. Training of Destruction Personnel. Contractors must ensure that destruction personnel have been properly trained prior to performing destruction. The personnel involved must be instructed on the proper use/handling of the destruction devices and the proper destruction procedures.

99. Procedures for Routine Destruction of COMSEC Material. Routine destruction should normally be done by the COMSEC Custodian and the Alternate COMSEC Custodian. However, this restriction should not be enforced at the cost of delaying destruction. Granting the authority to destroy superseded material to additional appropriately cleared 2/ people, who then certify this destruction to the COMSEC Custodian, is preferable to delaying destruction, even for short time. The following paragraphs indicate various types of procedures which might be followed in representative situations, with emphasis on keying material.

a. In a large facility, cleared users may be granted authority to destroy keying material they use, in the presence of cleared witnesses, as soon as the material is superseded.

b. In a small facility with only a few COMSEC equipments, the COMSEC Custodian may personally collect superseded keying material, replace it with new material, and effect timely destruction of superseded material in the presence of a cleared witness.

1/ DO NOT DESTROY defective or faulty keying material. Such material should be reported to DIRNSA, ATTN: S042, and held for disposition instructions.

2/ The term “appropriately cleared” and “cleared” means possession of a final security clearance equal to the highest classification of the material to be destroyed.

c. In mobile situations, routine destruction may be accomplished by the user and an appropriately cleared witness. The issuing COMSEC Custodian must be advised by the user, either verbally or in writing, that the user has destroyed the material. Verbal notification must be followed up with written confirmation of destruction as soon as possible. For accounting purposes, the COMSEC Custodian will then consider the material destroyed. In such cases, the COMSEC Custodian must brief the user on the necessity for prompt and complete destruction of superseded keying material, and for prompt reporting of any loss of control of material before destruction could be accomplished.

d. Scheduling Routine Destruction.

(1) Keying material designated CRYPTO which has been issued for use must be destroyed as soon as possible after supersession, and may not be held longer than 12 hours following supersession. However, where special circumstances prevent compliance with the 12-hour standard (e.g., facility unmanned over weekend or holiday period), the FSO may authorize an extension to a maximum of 72 hours. Keying material designated CRYPTO which has been issued for use must be destroyed as soon as possible after supersession, and may not be held longer than 12 hours following supersession. However, where special circumstances prevent compliance with the 12-hour standard (e.g., facility unmanned over weekend or holiday period), the FSO may authorize an extension to a maximum of 72 hours. Where communications activity is suspended for extended periods (e.g., plant-wide holidays), unused keying material need not be destroyed as it is superseded, but may be retained in the COMSEC account until communications activity resumes, at which time superseded key must be expeditiously destroyed. For circumstances not covered above, contact your COR for instructions.

(2) Complete editions of superseded keying material designated CRYPTO which are held by a user COMSEC account must be destroyed within 5 days after supersession.

(3) Maintenance and sample keying material not designated CRYPTO is not regularly superseded and need only be destroyed when physically unserviceable.

(4) Superseded classified COMSEC publications which are held by a user COMSEC account must be destroyed within 15 days after supersession.

(5) The residue of entered amendments to classified COMSEC publications must be destroyed within 5 days after entry of the amendment.

100. Routine Destruction Methods. The authorized methods for routinely destroying paper COMSEC material are burning, pulverizing or chopping, crosscut shredding, and pulping. Nonpaper COMSEC material authorized for routine destruction must be destroyed by burning, chopping or pulverizing, or chemical alteration.

a. Paper COMSEC Material. The criteria given below apply to classified COMSEC keying material and media which embody, describe, or implement a classified cryptographic logic. Such media include full maintenance manuals,

cryptographic descriptions, drawings of cryptographic logics, specifications describing a cryptographic logic, and cryptographic software. Other paper COMSEC material may be destroyed by any means that are approved for the destruction of other paper material of equal classification or sensitivity.

(1) When destroying paper COMSEC material by burning, the combustion must be complete so that all material is reduced to white ash, and contained so that no unburned pieces escape. Ashes must be inspected and, if necessary, broken up or reduced to sludge.

(2) When pulping, pulverizing, or chopping devices are used to destroy paper COMSEC material, they must reduce the material to bits no larger than five millimeters in any dimension.

NOTE : DO NOT PULP paper-mylar-paper key tape or high wet strength paper (map stock) and durable-medium paper substitute (e.g., TYVEC olefin,polyethlyne fiber) . These materials will not reduce to pulp, and must be destroyed by burning, pulverizing or chopping, or crosscut shredding.

(3) When crosscut (double cut) shredders are used to destroy paper COMSEC material, they must reduce the material to shreds not more than 3/64-inch (1.2 mm) in width and not more than l/2-inch (13 mm) in length, or not more than l/35-inch (0.73 mm) in width and not more than 7/8-inch (22.2 mm) in length.

b. Nonpaper COMSEC Material. The authorized methods for routinely destroying nonpaper COMSEC material are burning, melting, chopping, pulverizing, and chemical alteration. The material must be destroyed to the extent that there is no possibility of reconstructing classified information by physical, chemical, electrical, optical, or other means.

(1) Microforms (microfilm, microfiche, or other reduced-image photo negatives) may be destroyed by burning or by chemical means, such as emersion in household bleach (for silver film masters), or acetone or methelyne chloride (for diazo reproductions) for approximately five minutes. When destroying by chemical means, film sheets must be separated and roll film must be unrolled. NOTE : Caution should be exercised to prevent potential hazards when using chemical means for destruction. Contractors are also responsible for ensuring that OSHA standards are met.

(2) Magnetic or electronic storage or recording media are handled on an individual basis. Magnetic tapes may be destroyed by disintegration or incineration. Magnetic cores may be destroyed by incineration or smelting. Magnetic discs, disc packs, and drums may be destroyed by removal of the entire recording surface by means of an emery wheel, disc sander, or by incineration.

WARNING

DO NOT INCINERATE MAGNETIC TAPE ON ALUMINUM REELS, AS THIS MAY CAUSE AN EXPLOSION

(3) Hardware keying material (i.e., USKAU (Proms), USKAW (permuting plugs)) and associated manufacturing aids will not be destroyed without the approval of NSA.